UNITED STATES DISTRICT COURT

for the

Central District of California

FILED
CLERK, U.S. DISTRICT COURT
MAY - 1 2019
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

United States of America

v.

TIBO LOUSEE, KLAUS-MARTIN FROST, and JONATHAN KALLA,

Defendants

Case No. 19MJ1843

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the dates of October 2016 to April 2019 in the county of Los Angeles in the Central District of California, the defendants violated:

Code Section	*Offense Description*
21 U.S.C. §§ 846, 841(a)(1), (b)(1)(A)(viii), 18 U.S.C. § 1956(h)	See attached affidavit

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

for [signature]
Complainant's signature

Leroy Shelton, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 5/1/19

[signature]
Judge's signature

City and state: Los Angeles, California

Hon. Patrick J. Walsh, U.S. Magistrate Judge
Printed name and title

AUSA Ryan White, Cyber & Intellectual Property Crimes Section
AUSA Puneet V. Kakkar, International Narcotics, Money Laundering, & Racketeering Section
SAUSA Grant Rabenn (E.D. Cal.), Special Prosecutions Unit
DOJ Trial Attorney Alden Pelker, Computer Crime & Intellectual Property Section

Contents

AFFIDAVIT

I, Leroy Shelton, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint and arrest warrants for TIBO LOUSEE, also known as ("aka") "coder420," aka "codexx420" ("LOUSEE"); JONATHAN KALLA, aka "Kronos" ("KALLA"); and KLAUS-MARTIN FROST, aka "TheOne," aka "The_One," aka "dudebuy" ("FROST") (collectively known as "The Administrators") for violations of 18 U.S.C. § 1956(h) (conspiracy to launder monetary instruments) and 21 U.S.C. §§ 841(a)(1), (b)(1)(A)(viii), and 846 (distribution and conspiracy to distribute controlled substances) (the "Subject Offenses").

2. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses, including foreign law enforcement personnel. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND FOR LEROY SHELTON

3. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") and have been so employed since 2012. I

am currently assigned to the Los Angeles Field Office, Cyber Crime Squad, which is responsible for investigating computer and high-technology crimes. During my career as an FBI SA, I have participated in numerous cyber-related investigations. During the investigation of these cases, I have participated in the execution of numerous arrests, search warrants, and seizures of evidence. Since my assignment to the Cyber Crime Squad, I have received both formal and informal training from the FBI regarding cyber investigations. Through these means, I have learned about schemes and designs commonly used to commit financial- and technology-based crimes, as well as the practices that individuals who commit financial- and technology-based crimes employ while attempting to thwart law enforcement's efforts to effectively investigate those crimes.

III. RELEVANT DEFINITIONS

4. Based upon my training, experience, and research, I know that:

a. The Internet is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between Internet computers exist across state and international borders; therefore, information sent between two computers connected to the Internet frequently crosses state and international borders even when the two computers are located in the same state.

b. Individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet email accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them.

c. An Internet Protocol address ("IP address") is a unique numeric address used by each computer on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178), or a series of eight groups of four hexadecimal digits, with the groups separated by colons (e.g., 2001:0db8:0000:0042:0000:8a2e:0370:7334). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a range of IP addresses.

d. When a customer logs into the Internet using the service of an ISP, the computer used by the customer is assigned an IP address by the ISP. The customer's computer retains that IP address for the duration of that session (i.e., until the

user disconnects), and the IP address cannot be assigned to another user during that period.

e. Email, also known as “electronic mail,” is a popular means of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is initiated at the user’s computer, transmitted to the subscriber’s mail server, and then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.

f. The Tor network is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true IP addresses of the computers accessing the network, and, thereby, the locations and identities of he network’s users. Individuals who use Tor generally can remain anonymous to the destination server by routing their Internet traffic through the Tor network. Tor is made up of a decentralized network of computers or “nodes,” which relay traffic anonymously from the source node (i.e., the computer sending data), to the destination node (i.e., the computer receiving data). When Tor is used as an intermediary to route data, the path that the data can take is completely random, and the number of nodes that the data goes through before reaching the destination can vary. The nodes that relay the data within the Tor network from the source to the destination are called “relay nodes,” while the final node in the Tor network, which

sends the data to the destination computer, is called an "exit node." The data is encrypted from the time it leaves the source node, until it leaves the exit node and is finally forwarded to the destination computer. Tor requires that specialized software be downloaded and installed on the source node (i.e., the target's computer) to allow the data sent from the source node to be routed through the Tor network. Once the Tor software is installed, other Internet software on the source node computer (for example, a web browser) must be configured to use Tor, and thus to remain anonymous. Tor likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such "hidden services" operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software designed to access the Tor network.

g. "Darknet" and the term "dark web" refer generally to network(s) not accessible on the "surface web," which is what the layperson understands to be the Internet. Specifically, darknet websites such as Silk Road, AlphaBay and Hansa were infamous darknet markets operating on the Tor network.

h. Through the dark web or "darknet," i.e., websites accessible only through anonymity-enhancing networks such as Tor, individuals have established online marketplaces, such as the Silk Road and AlphaBay, for narcotics and other illegal items. These markets often only accept payment through virtual

currencies, such as Bitcoin. These markets usually have escrow accounts, through which consumers deposit their virtual currency for an orders placed on the marketplace; the funds are released to the vendor upon acknowledgement from the consumer that the good(s) purchased were received. The escrow account then accepts a fee for each transaction, which in turn goes to the operator of the darknet marketplace and serves as a commission and/or payment for the operation of the darknet marketplace.

i. Darknet marketplaces usually exist for finite periods of time. Over the past few years, law enforcement agencies have seized certain marketplaces, such as the Silk Road, AlphaBay, and Hansa. Accordingly, operators of darknet marketplaces take steps to avoid law enforcement detection. Furthermore, darknet marketplaces have ceased to exist because administrators have conducted “exit scams,” that is, chosen to immediately shut down the marketplace while the marketplace possesses a significant amount of money for pending orders belonging to users of the marketplace, thereby keeping the money for their own use.

j. Virtual currency is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Virtual currency is not issued by any government, bank, or company and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Virtual currency is not illegal in the United States and may be used for legitimate

financial transactions. However, virtual currency is often used for conducting illegal transactions, such as the sale of controlled substances.

k. Bitcoin is a type of virtual currency. Bitcoin payments are recorded on a public ledger (known as the "Blockchain") that is maintained by peer-to-peer verification, and is thus not maintained by a single administrator or entity. Individuals can acquire bitcoin either by "mining" or by purchasing bitcoin. An individual can "mine" for bitcoin by allowing his/her computing power to verify and record the bitcoin payments into a public ledger. Individuals are rewarded for this by being given newly created bitcoin.

i. An individual can send and/or receive bitcoin through peer-to-peer digital transactions or by using a third-party broker. Such transactions can be done on any type of computer, including laptop computers, tablets, and smart phones.

ii. Bitcoin are stored in or accessed through digital "wallets." A digital wallet stores the access code that allows an individual to conduct Bitcoin transactions on the public ledger. Many companies offer wallet services, such as Coinbase, Copay, and Blockchain. Even though the public addresses of those engaging in Bitcoin transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, it would be possible to determine what transactions

were conducted by that individual or entity. Bitcoin transactions are, therefore, described as "pseudonymous."

l. The term "public key" refers to Pretty Good Privacy ("PGP") encryption. Based on my training and experience, I know that PGP is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting text, e-mails, files, directories, and whole disk partitions as well as increasing the security of e-mail communications. PGP was developed by a software engineer in 1991 who wanted a way to transfer information securely over the Internet. Today, PGP is implemented throughout the public and private sector to help secure sensitive data transfers and communications. PGP in its most simplistic form consists of a person using a PGP tool to create a PGP key pair. The PGP key pair contains both a public key (to lock/encrypt the message) and a private key (to unlock/decrypt the message). In the event a person wanted to send a secure message to a friend, that person would send his/her public key to the friend, in which the friend could then encrypt a sensitive message with their own public key and send it back encrypted. The person receiving the sensitive message would then decrypt the message with his/her private key. Thus, the public key component can serve as an identifier for that individual, allowing others to communicate with that individual. Based on my training and experience, individuals are likely to retain the same PGP key pair over time and across platforms, because keeping the same key pair enables

the user to decrypt old messages and to continue existing lines of communications. There is generally no logical reason for a person to allow another person to use his/her public key, as it is only usable with the matching private key. With respect to the context of investigations involving the darknet, individuals are known to retain the same PGP key pair as an identifier across marketplaces and forums to signify that they are the same individual, despite any change in moniker.

m. Though Bitcoin transactions (and certain other virtual currencies) are traceable on the Blockchain, transactors can send virtual currency by using the services of "tumblers," or "mixers," which are services that commingle virtual currency assets before remitting them to a recipient. The use of "tumblers" and "mixers" are used to hide the original source of funds.

IV. SUMMARY OF PROBABLE CAUSE

5. Since July 2017, the Federal Bureau of Investigation, in conjunction with other agencies, including the Drug Enforcement Administration ("DEA"), United States Postal Inspection Service ("USPIS"), Internal Revenue Service ("IRS"), and Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"), has investigated Wall Street Market ("WSM"), a darknet marketplace known to host the trafficking of illegal narcotics, malicious software, stolen financial data, counterfeit goods, and other contraband through the Internet (Tor) and the United States mail. As part of this investigation, as more fully described below, law enforcement

has identified LOUSEE, KALLA, and FROST as the administrators of WSM, that is, those responsible for the operation and maintenance of the entire website/marketplace, which was largely run from servers based in Germany. As described below, the United States has worked with foreign counterparts in Germany and the Netherlands to identify LOUSEE, KALLA, and FROST, and German authorities arrested LOUSEE, KALLA, and FROST on or about April 23 and 24, 2019. This affidavit seeks permission to obtain warrants for U.S.-based charges against these three administrators of WSM.

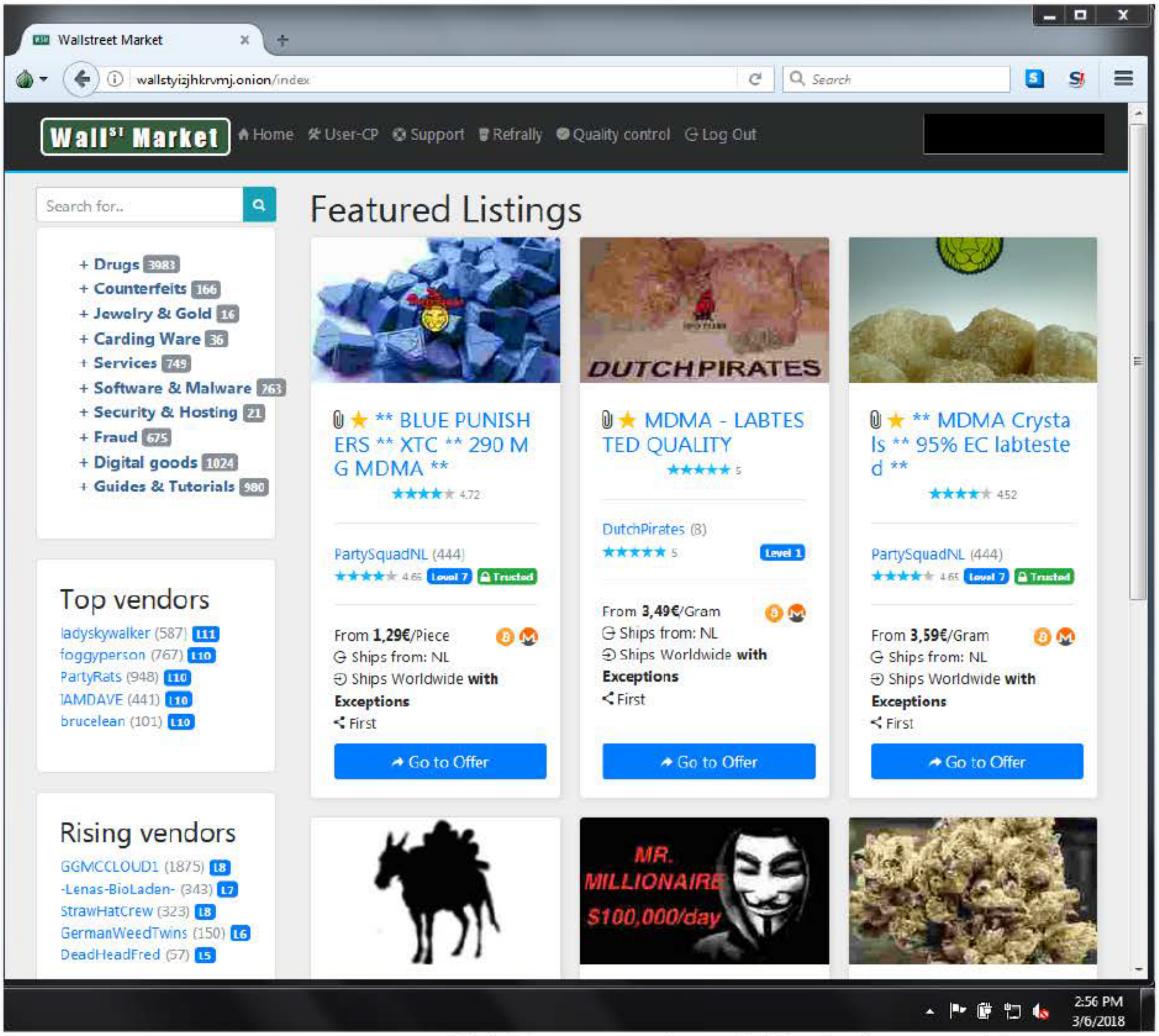
V. STATEMENT OF PROBABLE CAUSE

A. Overview of Wall Street Market ("WSM")

6. From approximately 2016 to 2019, as described herein, WSM was a darknet marketplace where vendors advertised and marketed the sale of illegal narcotics, malicious software, stolen financial data, counterfeit goods, and more. As of April 22, 2019, WSM was one of the largest and most voluminous darknet marketplaces of all time, made up of approximately 5,400 vendors and 1,150,000 customers around the world, as advertised and posted on the WSM homepage. As described more fully below, WSM has been placed in "Maintenance Mode" by German authorities (and therefore is non-operational), after arresting suspected administrators, LOUSEE, KALLA, and FROST.

7. WSM operated like a conventional e-commerce website, such as eBay and Amazon. However, its sole existence was geared to the trafficking of contraband. Based on my review of WSM,

including as an undercover consumer and vendor, I am aware of the following:



a. WSM was a "hidden service," that is, a site on the darknet, accessible only by programs such as Tor.

b. WSM's interface was available in six different languages: English, German, Spanish, French, Portuguese, and Italian.

c. WSM buyers were required to register for a free account by selecting a unique user name (otherwise known as a

moniker) and password. Once an account was created, users were able to browse goods for sale from the home page, which were organized by specific categories. Some of the categories included “Drugs,” “Counterfeits,” “Jewelry & Gold,” “Carding Ware,” “Services,” “Software & Malware,” “Security & Hosting,” “Fraud,” “Digital Goods,” and “Guides & Tutorials.”

d. WSM buyers were able to make purchases of contraband and illegal services on WSM and usually received physical contraband through the United States Mail and/or other means of physical delivery, such as commercial couriers and encrypted file-share programs.

e. WSM also provided a search function that allowed users to conveniently locate listings for the types of illegal goods or services they would want to purchase, and permitted searching by price range, popularity of item, vendor ratings, origin or shipping country, and payment type.

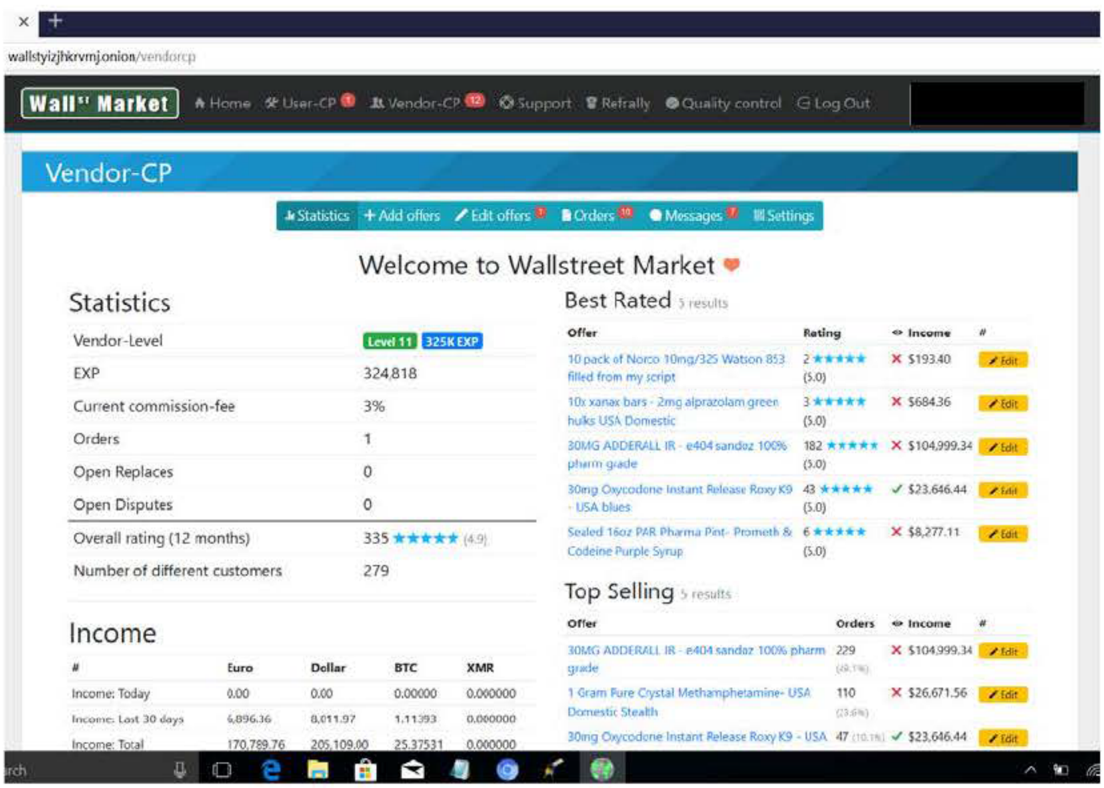
f. WSM also operated a forum (“the WSM Forum”), allowing users to discuss WSM-related matters. The forum was maintained and operated by a moderator(s), whose responsibilities included responding to any questions related to WSM among other things.

g. WSM required its users to trade in virtual currencies, primarily Bitcoin and Monero,[1] and the site did not allow for transactions in official, government-backed fiat currency. Because virtual currencies can be exchanged and

[1] Monero is another virtual currency, which, unlike Bitcoin, does not have a publicly viewable blockchain.

transferred peer-to-peer, users who use virtual currencies can limit their interaction with traditional, regulated financial institutions, which are required to collect information about their customers and maintain anti-money laundering and fraud detection measures. WSM and its users were therefore able to bypass the traditional financial systems by only permitting virtual currencies as a means of payment.

h. WSM sellers (also known as vendors) were required to pay for their vendor account and were provided a vendor webpage profile on WSM, akin to a storefront, where a vendor could advertise contraband. Vendors were given access to edit their webpage after logging into WSM. A vendor webpage included vendor statistics, listings of their contraband, and the ability to track the vendor's statistics and income generated over the



course of the account’s existence. WSM assisted buyers and vendors with instructions as to how to purchase such contraband and/or how it would be dispatched by the vendor.

i. Vendors on WSM received ratings from buyers, based on, among other things, the quality of contraband, reliability of delivery, and volume of traffic. In addition, WSM assessed rankings for vendors based on user input.

j. For each sale of contraband on WSM, WSM obtained a commission, ranging from approximately 2-5% of each transaction fee, dependent upon the vendor’s status and/or rating.

k. WSM provided security features for users and vendors. For example, WSM offered a platform for users to communicate with vendors with the option to encrypt their communications, such that only those parties involved could read the messaging between them.

8. Based on having witnessed undercover purchases of contraband on WSM and my knowledge of this investigation, I am aware of the following regarding customer purchases of contraband on WSM:

a. The customer selected contraband to purchase from a vendor and sent the vendor an order request.

b. The vendor acknowledged the customer’s order request and agreed to sell the contraband to the customer.

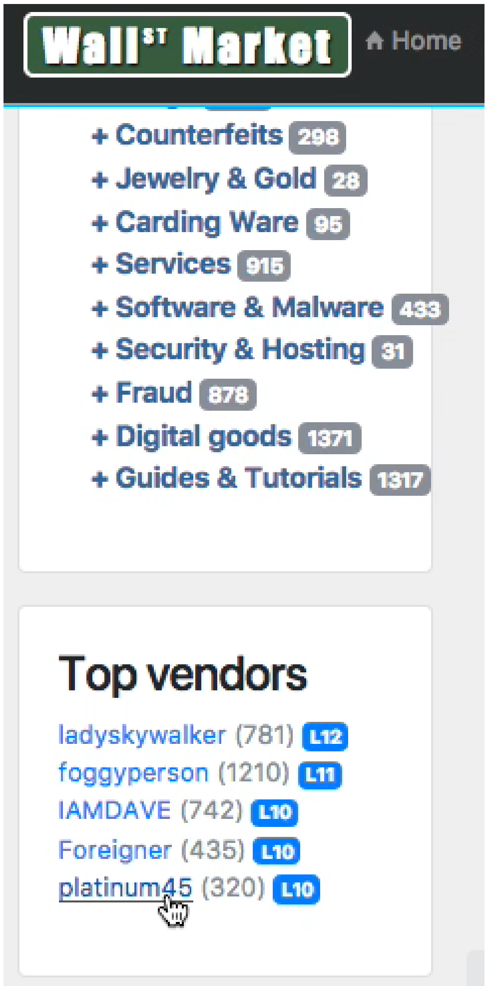
c. The customer sent money to the vendor, through WSM (usually to a unique payment address WSM generated for every transaction).

d. Usually after the vendor confirmed on WSM that the contraband had been shipped, WSM released the funds to the vendor for payment from the customer, less commission fees retained by WSM. (However, in some circumstances users would send the vendor funds prior to confirming contraband had actually been shipped.)

9. Based on my training and experience, the creation, operation, and maintenance of websites, and specifically, darknet marketplace websites such as WSM, require individuals to conceptually design a website that functions properly and provides a seamless user experience, much like most e-commerce websites. Once conceptualized, the individuals have to write the computer code (in this instance, WSM was written in the programming language PHP) to design the website and all the functionalities for each feature offered (such as the ability to create vendor and buyer accounts, compile and associate user accounts and passwords, track and manage orders, confirm shipments, and dispense funds to all parties, offer private communications, etc.), and maintain the daily operation of the website on remote computer servers. In this case, the WSM administrators created, maintained, and operated WSM and were responsible for, among other things, ensuring that vendor pages functioned properly (e.g., vendors could post pictures of contraband to advertise their products), the overall website functioned properly, and that transactions for contraband were properly processed (e.g., users could pay for contraband,

vendors could receive money, and the marketplace received its commission).

B. <u>Platinum45 and Ladyskywalker Were Major Drug Vendors on WSM in the Central District of California</u>



10. In or around September 2018, based on my review of WSM, I was aware that two of the top five vendors identified as "Top Vendors" on the WSM homepage included "ladyskywalker" and "Platinum45." I am aware that both of these vendors were operating in the Central District of California.

11. I have spoken with colleagues within the FBI, who arrested the individual responsible for operating the moniker "ladyskywalker." I am aware of the following based on my conversation with agents from the FBI leading this investigation:

a. "Ladyskywalker" operated on several darknet marketplaces, including WSM, and advertised and sold contraband on WSM such as fentanyl, oxycodone, and hydrocodone. "Ladyskywalker" sold these substances illicitly and to customers throughout the United States.

b. After receiving orders on WSM, which "ladyskywalker" accessed in the Central District of California, "ladyskywalker" would mail controlled substances by U.S. mail,

using fictitious return mailing addresses and in methods to avoid law enforcement detection.

c. WSM retained commissions for sales that "ladyskywalker" made on WSM.

12. I have participated and spoken with colleagues with DEA Los Angeles Field Office (Riverside), who arrested the individual responsible for operating the moniker "Platinum45." I am aware of the following based on my experience in the investigation and through conversations with DEA agents leading this investigation:

a. "Platinum45" operated on at least two darknet marketplaces, including WSM, and advertised and sold contraband on WSM such as methamphetamine, adderall, and oxycodone to customers around the world, including to Germany and Australia. "Platinum45" obtained prescription drugs from illegal prescriptions, pressed his/her own Adderall, and obtained methamphetamine from sources of supply in Southern California. "Platinum45" had advertised to sell up to 1,000 grams of methamphetamine on WSM.

b. After receiving orders on WSM, accessed in the Central District of California, "Platinum45" would mail controlled substances by U.S. mail, using fictitious return mailing addresses and in methods to avoid law enforcement detection.

c. WSM retained commissions for sales that "Platinum45" made on WSM.

C. Death Resulting from Distribution of Fentanyl

13. I have reviewed an affidavit from the Western District of Wisconsin in support of a complaint against a darknet vendor, and have learned the following:

a. In December 2017, a resident of Florida died as a result of a nasal spray laced with fentanyl that the decedent had ordered and received by mail. The United States Postal Inspection Service investigated the package in which the nasal spray arrived, and learned that similar packages of nasal spray laced with fentanyl were being sent to other locations. Further investigation revealed that these packages came from a vendor, "U4IA," who advertised on WSM. Law enforcement executed a search warrant at the residence of the individual operating as "U4IA" and seized, among other things, fentanyl, spray bottles, and a list of customer addresses. Based on my review of the docket for the case, I learned that this darknet vendor had been convicted for distributing fentanyl resulting in the overdose death of the Florida resident and was sentenced to 12 years in prison.

D. Other Contraband Purchased by Undercover FBI Agents

14. On or about October 19, 2017, an online covert employee ("OCE") for the FBI, acting in an undercover capacity in Los Angeles, California, purchased from a vendor on WSM a "fullz," which refers to a complete set of identifiers (name, date of birth, Social Security number, address, and credit card number), for an individual living in the Los Angeles area. The vendor, known as "DavidCVV," sent the fullz to the OCE through

an encrypted file-share application. I verified that the fullz information sold by the WSM vendor to the OCE was accurate and belonged to a real person living in Los Angeles, California.

15. On or about September 23, 2018, an OCE for the FBI, acting in an undercover capacity in Buffalo, New York, purchased from a vendor on WSM known as "Professor Dark," malware called "Spytech SpyAgent Keylogger." This keylogger was designed to log keystrokes from a computer infected with the malware.

E. Wall Street Market Was a Successor Market to German Plaza Market

16. Based on my discussions with a United States Postal Inspector who has been conducting virtual currency analysis related to WSM, I am aware of the following:

a. German Plaza Market ("GPM"), which launched in approximately Spring 2015, was a darknet marketplace (through which users transacted in Bitcoin) and shut down due to an "exit scam" in approximately May 2016.

b. Based on analysis of the Bitcoin Blockchain, during the time GPM was operational, a wallet referred to as "Wallet 2" received approximately 3,374 Bitcoin from funds believed to be associated with GPM.[2] Further analysis of the Bitcoin Blockchain reveals that, prior to the creation of GPM,

[2] References to wallets "associated" with darknet marketplaces derive from a proprietary program that analyzes financial transactions on the Blockchain (the public-facing online ledger of Bitcoin transactions) and that can identify groups of addresses that associate with darknet marketplaces. Law enforcement has used proprietary services offered by Blockchain analysis companies to investigate Bitcoin transactions. Through numerous unrelated investigations, the analytics tool provided by the company here has been found to be reliable.

in or around May 2015, Wallet 2 sent Bitcoin to another wallet, referred to as "Wallet 1."

c. Additionally, the last known transfer from wallets associated with GPM went to Wallet 2. Thus, based on this information, Wallet 2 is believed to be associated with the operators of GPM.

d. Based on analysis of the Bitcoin Blockchain, between February 2015 and March 2016, during which time GPM was operational, approximately 206 Bitcoin[3] was transferred from Wallet 2 to Wallet 1.

e. In or around August 2016, Wallet 2 sent Bitcoin to a third wallet, denoted here as Wallet 3, from which, in or around September 9, 2016, four transfers of Bitcoin were sent to a wallet associated[4] with WSM, which constituted the first identifiable transactions on the Blockchain associated with WSM.

f. Therefore, based on the training, experience, and knowledge of the team investigating the virtual currency transactions described herein, I believe that the administrators of GPM are also the administrators of WSM. After GPM administrators conducted an exit scam in May 2016, the Bitcoin wallet associated with GPM (Wallet 2) funded Wallet 3, which in turn funded a wallet associated with WSM before WSM became operational in October 2016. Therefore, this pattern means that the administrators of GPM likely transferred funds stolen from

---

[3] Based on my review of coinmarketcap.com, between February 2015 and March 2016, Bitcoin exchanged for $225 to $530.

[4] The proprietary program, described above, identified these wallets as those associated with WSM.

GPM to WSM, and then launched WSM. This belief is supported by KALLA's admission, discussed in paragraph 33.b below, that he and "coder420" (LOUSEE) and "TheOne" (FROST) were the former administrators of GPM.

F. Dutch and German Authorities Identify and Review the Infrastructure of WSM

17. In the course of this investigation, the U.S. government collaborated with law enforcement from countries where the infrastructure for WSM was believed to be operating. Pursuant to a request for multilateral assistance from the United States, in or around April 2018, the Netherlands imaged a server in its country, believed to be the server hosting and/or processing virtual currency transactions for WSM. I reviewed a copy of that server (the "WSM Virtual Currency Server"). Based on my review, I believe that this server was in fact part of the WSM infrastructure, because, among other reasons, I found the following references embedded in the code of various files:

a. "Wall Street Market // created by the talented, good-looking coder. #NoNameshere :P."

b. "'WSM_BTC,' 32Eurp1...[]"

c. SQL $db_name="tulpenland"[5]

18. Further, based on my review of the configuration ("config") file, which serves as a control file on the server, I identified IP addresses for the other servers that were a part

[5] Based on my training and experience, this means that the database name for a SQL server (that is, a server cataloging information) that is interacting with the server reviewed above is "tulpenland."

of the WSM infrastructure, including multiple IP addresses in Germany.

19. German law enforcement, specifically, the Bundeskriminalamt ("BKA"), which had been conducting its own investigation parallel to the investigations conducted by the United States and the Netherlands, had also reviewed the WSM Virtual Currency Server. The BKA then conducted an investigation into the IP addresses in Germany identified in paragraph 18 above, believed to be part of the WSM infrastructure.

20. In the course of BKA's investigation, and pursuant to valid legal process in Germany, the BKA identified the servers operating WSM. [redacted] Through valid legal process, the BKA imaged a copy of the database of WSM. The BKA has reviewed that database and confirmed that the database held information for WSM. I have also reviewed that database and confirmed that it is part of the infrastructure enabling WSM to operate. For example, in my review of the database imaged by the BKA, I observed that the SQL database was named "tulpenland."

21. In reviewing the WSM database, I reviewed the settings table. Based on my review of the settings table, I learned that it included conversations between The Administrators using the monikers "coder," "TheOne," and "Kronos." Those conversations are in German and discuss, among other things, WSM server

maintenance, concerns regarding vendors, and payments between The Administrators. Further, the settings table reveals that payments from WSM are split into three equal parts, one for each of The Administrators and paid once a month.

22. Additionally, the BKA advised me that in its analysis of the WSM infrastructure that was located in Germany, it found another server, located in the Netherlands, responsible for the development, testing, and updating of the WSM infrastructure (the “Gitlab server”). The Dutch National Police, in the course of its own investigation, and pursuant to valid legal process in the Netherlands, obtained an image of the Gitlab server. I also reviewed a copy of the image of the Gitlab server, and confirmed that it was part of the WSM infrastructure because of, among other things, the server contained programming code language for design, functionality, and maintenance of WSM. Additionally, I noted that there were three administrator accounts for the Gitlab server, with the following monikers: “coder420,” “TheOne,” and “Kronos,” which are similar to the administrative accounts identified in the settings table of the WSM database described in paragraph 21 above. Based on my training and experience, I know that separate administrator accounts on a development server, like the Gitlab server, signify multiple administrators with administrative rights and operational control over the Gitlab server and likely over the entire server infrastructure.

G. **The Administrators of WSM Are LOUSEE, KALLA, and FROST**

LOUSEE

23. During the BKA's investigation, the BKA determined the WSM administrators accessed the WSM infrastructure primarily through the use of two VPN[6] service providers. The BKA determined that one of the administrators (based on the fact that this individual was accessing control elements of WSM to which only an administrator had access) used VPN Provider #1. Based on the BKA's analysis of the WSM server infrastructure, the BKA noticed that on occasion, VPN Provider #1 connection would cease, but because that specific administrator continued to access the WSM infrastructure, that administrator's access exposed the true IP address of the administrator. The BKA then investigated the true IP address and relayed to me the following:

a. The BKA learned that the uncovered IP address belonged to a broadband, landline and mobile telecommunications company in Germany.

b. The individual utilizing the above-referenced IP address to connect to the WSM infrastructure used a device called a UMTS-stick[7] (aka surfstick). This UMTS-stick was registered to a suspected fictitious name.

24. Between January 17, 2019 and February 7, 2019, the BKA executed multiple surveillance measures to electronically locate

---

[6] VPN or Virtual Private Network is a connection method used to add security or privacy to private and public networks.

[7] UMTS-stick or UMTS-Modem are designed to connect to the internet via a mobile network.

the specific UMTS-stick. The BKA has advised me of the following, based on its surveillance measures: BKA's surveillance team identified that, between February 5 and 7, 2019, the specific UMTS-stick was used at a residence of LOUSEE in Kleve, Northrhine-Westphalia (Germany), and his place of employment, an information technology company where LOUSEE is employed as a computer programmer. As discussed in paragraph 33.a below, LOUSEE was later found in possession of a UMTS stick.

25. Investigators have also requested, through legal process, information related to LOUSEE and various internet service providers. This information corroborates LOUSEE's role as an administrator of WSM. For example, I am aware of the following:

a. According to the Dutch National Police, which issued legal process from Github, a platform for software and coding development sharing, LOUSEE holds an account with the user name "codexx420" similar to the administrator account "coder420" found on the Gitlab server.

b. According to results from Twitter and Apple that I have reviewed, obtained pursuant to U.S. court orders requiring such disclosures that I obtained, I found the following items:

i. Pictures referencing virtual currency such as Bitcoin and Monero;

ii. A picture referencing "Gitlab";

iii. A picture of a computer logged into a Gitlab account (unrelated to WSM) but related to LOUSEE's employment as a computer programmer;

iv. Pictures of LOUSEE consuming marijuana;

v. Numerous references to "420," including a license plate of LOUSEE's vehicle and a sign on a bedroom wall with "420."[8]

26. Based on the information above, I believe that LOUSEE was the administrator whose account was "coder420."

KALLA

27. The BKA also investigated a second individual suspected to be an administrator, who was using VPN Provider #2, to access certain administrator-only components of the WSM server infrastructure. The BKA advised me, based on its investigatory process, that it learned that an IP address assigned to the home of this individual (the account for the IP address was registered in the name of the suspect's mother) accessed VPN Provider #2 within similar rough time frames as administrator-only components of the WSM server infrastructure were accessed by VPN Provider #2. Based on my training and experience, I believe that this individual, later determined to be KALLA, accessed VPN Provider #2 to access administrator-only components of WSM server infrastructure.

28. As referenced below at paragraph 33.b, KALLA admitted that he was the administrator for WSM known as "Kronos."

---

[8] Based on my training and experience as an investigator, I am aware that "420" is a reference to marijuana.

FROST

29. The third administrator for WSM was known as "TheOne," and as described below, the investigation has further revealed probable cause to believe that FROST is "TheOne" for two primary reasons. First, as described below (at paragraph 30), the PGP public key for "TheOne" is the same as the PGP public key for another moniker on Hansa Market, "dudebuy." As described below, a financial transaction connected to a virtual currency wallet used by FROST was linked to "dudebuy." As explained above in paragraph 4.l, a PGP public key, in the context of darknet investigations, is likely a unique identifier to an individual. Second, as described below (at paragraph 31), investigators have identified a wallet used by FROST that subsequently received Bitcoin from a wallet used by WSM for paying commissions to administrators.

30. As mentioned above, FROST is believed to be "TheOne" because of a link between him and the "dudebuy" moniker on Hansa.

a. The BKA advised me that they located the PGP public key for "TheOne" in the WSM database, referred to as "Public Key 1".

b. Based on my conversation with the same United States Postal Inspector mentioned above in paragraph 16, I learned the following regarding FROST:

i. As reflected on an image of the Hansa Market (which was seized by law enforcement in 2017), Public Key 1 was

the PGP public key for “dudebuy.”[9] The “refund wallet” for “dudebuy” was Wallet 2.

ii. Wallet 2 was a source of funds[10] for a Bitcoin transaction that ultimately paid for services on October 15, 2016 at a company engaged in digital marketing (“Product Services Company”) via a payment processing company (“Bitcoin Payment Processing Company”). Records obtained from the Bitcoin Payment Processing Company revealed buyer information for that Bitcoin transaction as “Martin Frost,” using the email address klaus-martin.frost@web.de.[11]

iii. Prior to WSM opening in October 2016, FROST used funds from a Bitcoin wallet (referred to as “Wallet 4”) to pay for two accounts with a video game company (the “Gaming Company”), for accounts with email address klaus-

---

[9] This was ascertained by a review of data that was obtained from the Hansa Market server pursuant to its seizure in 2017.

[10] The United States Postal Inspection Service learned, through its analysis of Blockchain transactions and information gleaned from the proprietary software described above, that the funds from Wallet 2 were first transferred to Wallet 1, and then “mixed” by a commercial service; mixing services is described above at paragraph 4.m. Through thorough analysis, the United States Postal Inspection Service was able to “de-mix” the flow of transactions, to eventually ascertain that the money from Wallets 1 and 2 ultimately paid FROST’s account at the Product Services Company.

[11] The BKA advised me that this is the email address for FROST.

martin.frost@web.de,[12] via a Bitcoin Payment Processing Company.[13] After these transactions, Wallet 4 was funded by Wallet 2.

31. A second link connecting FROST to the administration of WSM is based on additional Bitcoin tracing analysis. Based on my conversations with the United States Postal Inspector conducting virtual currency analysis, I am aware of the following:

a. Prior to WSM opening in October 2016, on September 3, 2016, funds from a Bitcoin wallet (referred to as "Wallet 5") were used[14] to pay for another account with the Gaming Company, for an account with email address klaus-martin.frost@web.de,[15] via the Bitcoin Payment Processing Company.[16] After this transaction, Wallet 5 was later funded (for other transactions) by wallets "associated"[17] with The Administrators of WSM, that is, wallets receiving commissions

---

[12] This information came from subpoenaed records from the Gaming Company.

[13] Similar to the above, the funds from Wallet 4 were also "mixed" by a commercial service, and through thorough analysis, the United States Postal Inspection Service was able to "de-mix" the flow of transactions, to eventually ascertain that funds from Wallet 4 paid FROST's accounts at the Gaming Company.

[14] Similar to the above, the funds from Wallet 5 were also "mixed" by a commercial service, and through thorough analysis, the United States Postal Inspection Service was able to "de-mix" the flow of transactions, to eventually ascertain that funds from Wallet 5 paid FROST's account at the Gaming Company.

[15] This information came from subpoenaed records from the Gaming Company.

[16] Similar to the above, the funds from Wallet 5 were also "mixed" by a commercial service, and through thorough analysis, the United States Postal Inspection Service was able to "de-mix" the flow of transactions, to eventually ascertain that funds from Wallet 5 paid FROST's accounts at the Gaming Company.

[17] See footnote 2.

from WSM (which are unique to administrators, who receive commissions for transactions on the marketplace).

H. WSM Is Believed to Have Conducted an Exit Scam, Leading the BKA to Arrest Suspected Administrators LOUSEE, KALLA, and FROST in Germany

32. In or around April 2019, WSM experienced massive popularity and then commenced an "exit scam," presumably in response to its increased popularity. Based on reviewing open-source commenting on darknet forums, I am aware of the following:

a. On or about March 25, 2019, WSM became broadly regarded as the pre-eminent darknet marketplace because of the advertised shutdown of another competing darknet marketplace.

b. Shortly thereafter, WSM experienced an influx of new buyers and vendors, and its management team stated publicly that it needed to account for the growth by expanding server capacity.

c. On or about April 16, 2019, vendors on WSM could not withdraw funds from their escrow accounts; that is, they could not repatriate proceeds for contraband that was sold.

d. Between April 22 and 26, 2019, members of the public shared that their own analyses of virtual currency transactions revealed that large amounts of virtual currency, estimated between $10 and $30 million, were being diverted from wallets believed to be associated with WSM to other virtual currency wallets.

33. In response to the suspected exit scam, the BKA obtained, pursuant to German laws, various search and arrest

warrants related to LOUSEE, KALLA, and FROST. Based on my conversations with the BKA, I am aware of the following:

a. On the day of LOUSEE's arrest, before the BKA arrested LOUSEE, BKA observed a connection to WSM infrastructure (which is only done by administrators) from the UMTS-stick, and through electronic surveillance, determined that the UMTS-stick used to access the WSM infrastructure was at LOUSEE's residence at the time. Upon the execution of LOUSEE's arrest, the BKA noticed LOUSEE's computer was unlocked and located a UMTS-stick that is believed to have been used to log into WSM, as described in paragraphs 23-24 above.

b. KALLA was arrested, and, after being advised of his rights under German law, confessed to being an administrator of WSM, known as "Kronos." He admitted that he maintained a technical role with respect to WSM and identified the location of the WSM forum. He also admitted that he was involved in the administration and operation of a prior darknet marketplace, GPM (described in paragraph 16.a), along with "coder420" and "TheOne."

c. FROST was arrested.

VI. <u>CONCLUSION</u>

34. For all the reasons described above, there is probable

///

///

cause to believe that LOUSEE, KALLA, and FROST have committed violations of the Subject Offenses.

P J Walsh for

Leroy Shelton, Special Agent
Federal Bureau of Investigation

at 5:50 p.m.

Subscribed to and sworn before me this 1st day of May 2019, *

Patrick J. Walsh

HONORABLE PATRICK J. WALSH
UNITED STATES MAGISTRATE JUDGE

The agent ~~was~~ is in Germany; I am in Los Angeles. The Complaint and Warrants were subscribed and Sworn over the phone. The Court recorded the process and has instructed the agent to appear in person when he returns to the U.S. to endorse the affidavit in the Court's presence